

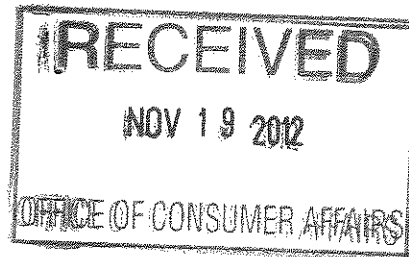


201 West Main Street, Suite 14
Charlottesville, VA 22902-5065
434-977-4090
Fax 434-977-1483
SouthernEnvironment.org

#3119

November 16, 2012

Undersecretary Barbara Anthony
Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116



Re: Notification of Security Breach

Dear Undersecretary Anthony:

Pursuant to M.G.L. c. 93H, the Southern Environmental Law Center (SELC), based in Charlottesville, VA, is writing to notify the Office of Consumer Affairs and Business Regulation that there has been a computer security breach of personal information affecting one Massachusetts resident.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On October 16, SELC learned that it had been the victim of an internet security breach in which highly confidential information was taken without our consent or authorization, and then circulated by email and posted on the internet. The date and reason the security breach occurred is currently under investigation by the Federal Bureau of Investigation; SELC estimates the breach took place the first half of October 2012 or late September. Initial investigation indicates it was an intentional malicious attack on our server. The categories of personal information involved in the incident include personnel files and materials submitted by applicants seeking employment with SELC. The personal information that was the subject of the incident was in electronic form.

NUMBER OF MASSACHUSETTS RESIDENTS AFFECTED

During the week of October 29, SELC—a regional organization that works in Virginia, Tennessee, North Carolina, South Carolina, Georgia, Alabama, and the District of Columbia—discovered that the security breach could have affected one Massachusetts resident, who had provided SELC with documents such as a law school transcript that may have included their social security number, when they applied for employment with SELC. This Massachusetts resident has received a notice pursuant to M.G.L. c. 93H, s. 3(b) via email. A copy of the notice is enclosed.

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

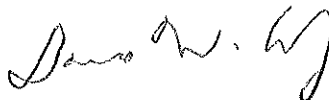
SELC has taken several steps to remedy the breach and restore the integrity of the system. When the incident was discovered, SELC reported the breach to the Federal Bureau of Investigation and requested successfully that the documents be removed from the internet. SELC has also assembled a team of SELC staff and outside consultants and experts to take all

necessary actions to address the breach and the unauthorized release of confidential information. Due to SELC's diligent efforts to remedy the breach, it appears that all of the confidential information disseminated on the internet was removed by October 18. There is no evidence at this time that the personal information has been used for fraudulent purposes. SELC will perform regular security audits and penetration tests to prevent a similar breach from occurring in the future.

OTHER NOTIFICATION AND CONTACT INFORMATION

SELC has provided a similar notification to the Office of the Attorney General. Please contact SELC by phone, at (434) 977-4090, or by email, at dcarr@selcva.org, if there are any questions

Sincerely,

A handwritten signature in black ink, appearing to read "David Carr", with a stylized flourish at the end.

David Carr
General Counsel

The Southern Environmental Law Center (SELC) was the victim of a major internet security breach discovered on October 16th in which highly confidential information was taken without our consent or authorization from our secure server, and made accessible on the internet for a limited time. (Some confidential information was also circulated by email.) Due to our extensive and immediate efforts, this confidential information was no longer available on the web as of the morning of October 18th. We reported the breach to the FBI on October 16th and their investigation is ongoing.

SELC has taken and will continue to take all necessary measures to prevent a similar breach from occurring in the future. Regular security audits will be performed, and penetration tests and internal auditing will be conducted to identify any future vulnerabilities and security risks. SELC has hired additional outside consultants to assist us in conducting these security audits and implementing their recommendations.

We have recently discovered that certain job applications kept on the server that was breached included transcripts that showed full social security numbers or a student ID that could be a social security number. We do not know if these transcripts were exposed, but it is possible they were. Your transcript included a social security number or an ID with nine digits that could be your SSN. **Therefore, we are writing to provide you notice that your social security number could have been exposed in the breach.** (You should check your transcript to see if it included your SSN- if not, you may not need to take the steps below unless your transcript number and name would allow access to your personal financial information.) We regret this potential exposure and recommend the following to help protect your credit.

We advise you to remain vigilant concerning your personal credit information. Even if you do not find any suspicious activity on your credit reports, you should check your credit reports periodically. **Order a free credit report** and review it for accuracy. See the contact information for the credit bureaus below.

You should also consider placing a fraud alert or security freeze on your credit file. A fraud alert requires creditors to contact you before they open any new accounts or change your existing accounts. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization.

We recommend you take the steps below to protect your credit:

- 1. Contact the fraud units of one of the three major credit reporting bureaus** to place an initial fraud alert- there is no charge for this service. **(You only need to contact one of the companies – they will alert the others)**

Equifax (800-525-6285)
Trans Union: (800-680-7289)
Experian: (888-397-3742)

2. You should contact your bank and credit card companies and follow their recommendations. Many credit card companies and banks have a fraud line that will help you ascertain if your accounts have been interfered with, and you can place a special fraud alert if there is any activity or evidence of someone trying to use your SSN.

3. Check your bank account routinely for unexplained withdrawals and **check your credit card accounts** for unexplained charges. Notify them immediately.

A Federal Trade Commission booklet on identity theft that provides comprehensive information is available using the following link:

<http://www.ftc.gov/bcp/edu/microsites/idtheft2012/>

4. If you have reason to believe that your information is being misused, you should contact local law enforcement (including your state attorney general's office) and file a police report, and in such an event, creditors may want a copy of a police report to absolve you of any fraudulent debts.

Contact information for the three major national credit bureaus is provided below, along with additional information for residents of specific states, but which may be of interest to you even if you are not a resident of the noted states.

Please contact Amy Day at aday@selcva.org or call the SELC main phone number at (434) 977-4090 if you have any questions regarding the disclosure.

Sincerely,

David W. Carr, Jr., General Counsel
Southern Environmental Law Center
201 West Main Street, Suite 14
Charlottesville, VA 22902-5065

Credit Bureau Information and Additional Notifications for Residents of Certain States

For residents of California, Hawaii, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia, and Wyoming:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. It is recommended by state law that you remain vigilant for incidents of fraud and identify theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.transunion.com

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about steps you can take to avoid identity theft.

**Maryland Office of the
Attorney General**

Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

**North Carolina Office of the
Attorney General**

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)

www.ftc.gov/bcp/edu/microsites/idtheft/

For residents of Illinois:

It is required by state law to inform you that you can obtain information from the national consumer reporting agencies and the Federal Trade Commission about fraud alerts and security freezes.

For residents of Massachusetts and West Virginia:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$10.00 (depending on where you reside) to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

Equifax Security Freeze

Experian Security Freeze

TransUnion

P.O. Box 105788
Atlanta, Georgia 30348
www.equifax.com

P.O. Box 9554
Allen, TX 75013
www.experian.com

P.O. Box 6790
Fullerton, CA 92834
www.transunion.com